BRINGING ORDR TO CMMC COMPLIANCE FOR UNMANAGED DEVICES

INTRODUCTION

The Cybersecurity Maturity Model Certification (CMMC) defines a particularly broad set of security requirements that apply to virtually any organization that does business with the U.S. Department of Defense. Originally published in January of 2020, the CMMC Version 1.02 aims to bolster the security of the extended DoD supply chain, which has increasingly come under attack from a wide range of malicious actors. CMMC is expected to be implemented by more than 300,000 companies that make up the Defense Industrial Base (DIB) that provides support for the DoD.

The CMMC framework's overarching goal is to protect federal information that resides in an organization's environment, including Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Any computer or electronic device that processes federal data considered sensitive will need to be protected from the associated range of many threats. Organizations will need to consider a wide range of security best practices when developing their compliance strategies, including traditional managed devices, unmanaged devices, network, IoT and OT devices.

Many organizations today lack visibility, understanding and control of their devices as to what data or information is flowing in and out of their organization.

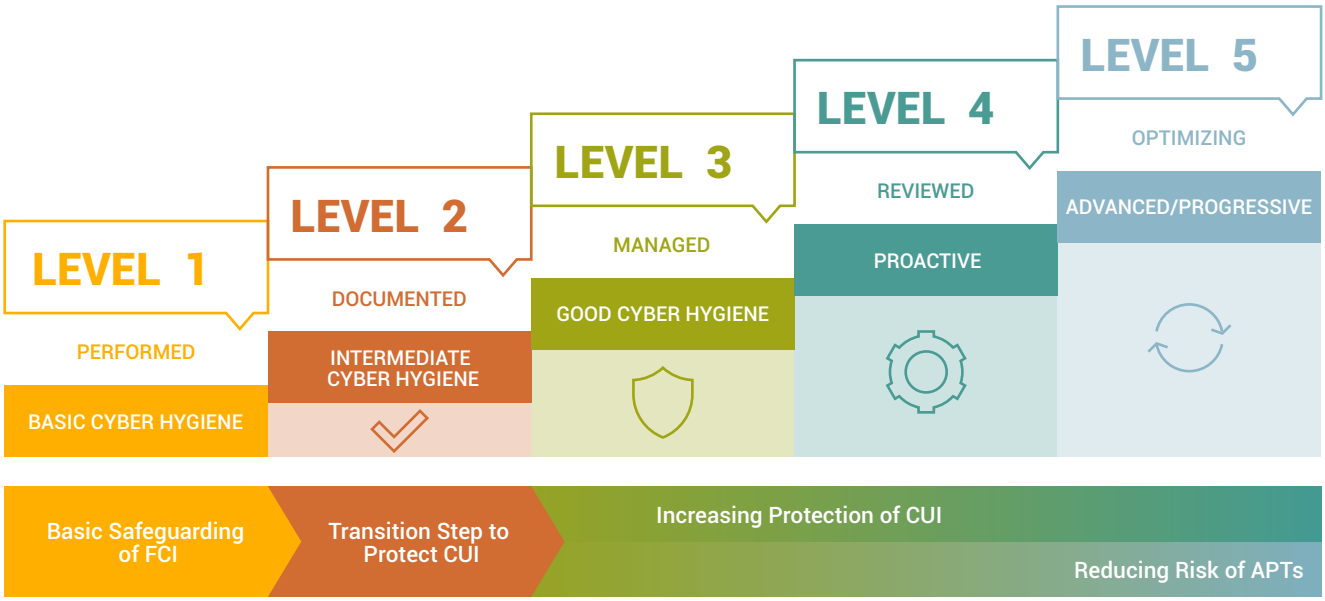
This paper shows how the Ordr Systems Control Engine (SCE) fills the gaps for CMMC requirements.

CMMC LEVELS

The CMMC is built on a multidisciplinary maturity model approach to security that aims to establish an overall security framework for DIB organizations. It is particularly broad in scope, covering a variety of security capabilities and best practices across 17 security domains. Domains include practices for technical controls implemented through hardware or software, such as vulnerability scanning and behavioral threat detection, Domains includes practices for organizational controls to develop policies, plans and the human aspects of security, such as security training and situational awareness.

CMMC recognizes that cybersecurity is not a one size fits all proposition. CMMC defines 5 levels of cybersecurity maturity providing a path to security improvement. For example, CMMC Level1 focuses on establishing basic levels of security hygiene to protect FCI, while Level 5 defines the most advanced measures designed to protect CUI from APTs.

CMMC LEVELS AND ASSOCIATED FOCUS



Source: Cybersecurity Maturity Model Certification ver 1.02

The required maturity level a particular organization will need to implement will vary based on a wide variety of factors, such as the size, scope, complexity, types of contracts and sensitivity of the data or information that needs to be protected based on the threats an organization faces.

"Asset Management" is an example of a security domain. A practice in the Asset Management domain, **AM.4.226**, defines the need to discover and identify systems with specific security related attributes

Let's examine CMMC specific practices where Ordr Systems Control Engine (SCE) will benefit you with a coordinated approach to the security of all your devices in a CMMC regulated environment.

APPLYING ORDR SCE TO CMMC REQUIREMENTS

This section reviews some of the specific CMMC domains and practices related to the security and management of devices in a DIB organization's environment. We then introduce ways that the Ordr SCE platform can potentially apply to these requirements.

ACCESS CONTROL (AC)

RELEVANT PRACTICES

AC.1.001 - Limit information system access to authorized users, processes, or devices

AC.1.002 - Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

AC.1.003 - Verify and control / limit connections to and use of external information systems

AC.4.023 - Control information flows between security domains on connected systems

AC.5.024 - Identify and mitigate unidentified access points connected to the network

HOW ORDR CAN HELP

The Ordr SCE analyzes the environment to discover and identify all connected devices including unmanaged, IoT, and OT devices. Each device is classified by its type or function (e.g. security camera) and the solution then gives details of the specific device down to the operating system and configuration. Ordr also learns the communication patterns for each device and the other systems it interacts with.

This visibility allows organizations to identify all devices, and in the process can reveal any potential rogue access points. Next, Ordr provides visibility into which devices are connecting to which systems and can generate enforcement policies to ensure that only necessary devices are allowed to connect to protected systems. This can provide appropriate isolation policies for devices and their services based on their sanctioned use and can provide additional critical context to support other access solutions such as a NAC deployment. Additionally, traffic analysis can reveal devices that are not employing appropriate levels of encryption.

ASSET MANAGEMENT (AM)

RELEVANT PRACTICES

AM.4.226 - Employ a capability to identify systems with specific component attributes (e.g. OS type)

HOW ORDR CAN HELP

Ordr automatically analyzes devices to reveal a variety of detailed device attributes. Depending on the device, this can include manufacturer, model, serial number, operating system traits, installed software, and a wide variety of connectivity traits.

CONFIGURATION MANAGEMENT (CM)

RELEVANT PRACTICES

CM.2.061 - Establish and maintain baseline inventories and configurations for organizational systems

HOW ORDR CAN HELP

Ordr's automated discovery of all connected devices allows organizations to ensure they always have an up to date inventory of their devices including the various types of unmanaged devices that are typically missed in traditional inventory efforts. The solution also delivers visibility into system and connectivity attributes which can be tracked over time.

INCIDENT RESPONSE (IR)

RELEVANT PRACTICES

IR.2.093 – Detect and report events

IR.2.094 – Analyze and triage events to support event resolution and incident declaration.

HOW ORDR CAN HELP

Ordr provides alerting of a variety of events including indicators of compromise as well as anomalous or suspicious device behavior. The platform additionally integrates with a variety of additional tools such as SIEMs and IT service management platforms to facilitate the response and resolution of events.

RISK MANAGEMENT (RM)

RELEVANT PRACTICES

RM.2.142 - Scan for vulnerabilities in organizational systems

RM.3.144 - Periodically perform risk assessments to identify and prioritize risks according to risk categories, risk sources, and risk measurement criteria.

RM.3.147 - Manage non-vendor-supported products separately and restrict as necessary to reduce risk

HOW ORDR CAN HELP

Ordr performs a continuous risk assessment of the environment based on observed vulnerabilities and threat-based indicators of risk. Ordr device discover is enriched with vulnerability database intelligence and optionally integrates with other 3rd party vulnerability scanners like Rapid 7 and Tenable. Integration with vulnerability management solutions such as Rapid7 and Tenable allow the Ordr dashboard to incorporate and present risk information from active network scans, while also sending important context to the vulnerability scanner itself. Ordr also ingests data from a variety of external sources such as industry-specific recall databases to identify devices that pose a particular risk. Devices that are recalled, vulnerable, or show signs of compromise can be automatically isolated based on company policy.

SECURITY ASSESSMENT (CA)

RELEVANT PRACTICES

CA.2.157 - Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

HOW ORDR CAN HELP

Ordr automatically builds a connectivity flow “genome” for each device. Ordr Flow Genom shows all the systems that a device communicates with including the types of traffic. In addition to showing the connectivity of systems, this visibility is mapped on top of Layer 2 and Layer 3 network topologies to show the devices in relation to VLANs and subnets. Communication of a device to the Internet, in particular to a malicious domain, is also highlighted as a risk.

SYSTEM COMMUNICATION AND PROTECTION (SC)

RELEVANT PRACTICES

SC.1.175 - Monitor, control, and protect organizational communications at external boundaries and key internal boundaries.

HOW ORDR CAN HELP

As described above, Ordr makes it easy to see exactly how all devices are communicating including traffic to and from the Internet or internal subnets. Communications to a risky or bad domain is identified as a security risk. Ordr can also automatically generate firewall policies to prevent unauthorized access, or alternately can provide staff with the necessary visibility to create policies on a case by case basis.

SYSTEM INTEGRITY (SI)

RELEVANT PRACTICES

SI.5.223 - Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.

HOW ORDR CAN HELP

In addition to monitoring devices for known signs of compromise such as communication with malicious domains or IP addresses, Ordr also monitors the behavior of all connected devices to identify signs of compromise. This can include behaviors that are out of the norm for a particular device type (e.g. HVAC system) or for the specific device in question. This can also identify systems that are attempting to masquerade a different device type such as a compromised laptop attempting to appear like an IoT device to evade security controls.

CONCLUSION

CMMC compliance will force many organizations to take a fresh look at their cybersecurity program and make changes to align with DoD requirements. Core security functions such as inventory, risk management, and threat detection will be essential to maintaining compliance, and organizations should look for efficient, automated systems that can help provide coverage for all connected devices including unmanaged, IoT, and OT devices. The Ordr SCE can arm organizations with a powerful tool to gain visibility into their environments including all their devices. The solution can then automatically expose potential risk, and enforce policies to either isolate high-risk devices, or to segment systems based on their unique needs. To learn more about Ordr and how the solution can help meet your compliance goals, contact the Ordr team at www.ordr.net.